Abstract

Over the last two decades, several applications of the theory of algebraic curves over finite fields to information sciences have been developed: for example, algebraic-geometric codes introduced by Goppa [**Gop81**], elliptic curve cryptography by Koblitz [**Kob87**] and Miller [**Mil86**], factorization of large numbers by Lenstra Jr. [**LJ87**], generating pseudorandom sequences by Xing and Lam [**XL99**], and so on. In this thesis, we present new applications of algebraic curves to the constructions of combinatorial designs and combinatorial arrays which are practically used in statistical experiments.

An *algebraic curve* is the set of zeroes (roots) of a polynomials. Each element of a curve is called a *point* on the curve. A curve is usually considered over an *algebraically closed field* $\bar{K}$ containing a field K, that is, the coordinates of the points on the curve may lie in $\bar{K}$ when the curve is defined by a polynomial over K. By considering over an algebraically closed field, we have a number of excellent results on algebraic curves, such as the result on the number of intersection points of two curves. In the theory of algebraic curves, the complex number field is often used as the ground field of curves. However an algebraically closed field containing a finite field is more suitable for applying the curves to information sciences. The union of all finite dimensional extensions of a finite field $\mathbb{F}_q$ is an algebraically closed field containing $\mathbb{F}_q$.

Suppose here that curves are defined by polynomials over a field K. A *divisor* is a formal sum $\sum_P m_P P$ of points on a curve with integral coefficients. A *rational function* is a quotient of two polynomials. It

is well known that a certain set of rational functions determined by a divisor forms a linear space over K. One of the applications of this linear space of rational functions is an algebraic-geometric code, which was originally introduced by Goppa [**Gop81**].

A point $P = (x, y)$ can be represented by a parameter t as $x = \sum_i x_i t^i$ and $y = \sum_i y_i t^i$. Hence the expansion of a rational function $f(x, y)$ at the point P has the form $f = \sum_i^\infty \alpha_i t^i$. For generating pseudorandom sequences, Xing and Lam [**XL99**] used the sequence $(\alpha_1, \alpha_2, \dots)$.

The fact that the point set on an elliptic curve forms a group is one of the most important results. The groups on elliptic curves are used in elliptic curve cryptography [**Kob87, Mil86**] and in factorization of large numbers [**LJ87**].

In this thesis, we will show some new applications of algebraic curves to the constructions of balanced arrays and balanced n-ary designs.

A balanced array is a combinatorial array whose entries are taken from a set S of symbols. When S is a subset $\{0, 1, \dots, s-1\}$ of non-negative integers, the balanced array is then an s-ary matrix.

Let V be a set of v elements and $\mathcal{B}$ a collection of (multi-)subsets of V. The pair $(V, \mathcal{B})$ is said to be a *block design*, while the elements of V and $\mathcal{B}$ are *treatments* and *blocks*, respectively. Although most of combinatorial designs have blocks which are subsets of the set V of treatments, some of them may have blocks which are multi-subsets. We often represent a block design by its *incidence matrix*. Each entry of the incidence matrix of a design is the number of occurrences of a treatment in a block. The incidence matrix of a design may not be binary if the design has blocks with repeated elements. A balanced n-ary design is a block design with repeated elements in blocks and it has an n-ary incidence matrix.

Let C and C' be two algebraic curves defined by polynomials F and F', respectively. An *intersection point* P of C and C' is a common

root of F and F', and the *intersection multiplicity* of P is defined to be the multiplicity of the root. The fundamental idea of our methods for constructing balanced arrays and balanced n-ary designs is to take the intersection multiplicity of two curves as the entry of an n-ary matrix.

In Chapter 1, we review the precedent applications of algebraic curves and the practical usages of balanced arrays and balanced n-ary designs. A brief overview of our new constructions for balanced arrays and balanced n-ary designs is also presented together with the definitions of these designs and arrays. Although an introduction of algebraic curves is given in Chapter 1, theory of algebraic curves used in our constructions is described rigorously in Chapter 2. As a new application of algebraic curves, some construction methods of balanced arrays are presented in Chapter 3. To construct balanced arrays, we need a *symmetric set of curves*. A part of Chapter 3 which discusses symmetric sets of curves is based on the paper [**FHS99**] by the present author with his supervisor Professor Ryoh Fuji-Hara. In Chapter 4 we describe a construction method of balanced n-ary designs, which is a modification of the constructions of balanced arrays in Chapter 3.